ASSEMBLÉE NATIONALE

17e LÉGISLATURE

Compte rendu

Commission spéciale chargée d'examiner le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité

Mardi 10 juin 2025
Séance de 16 heures 30

Compte rendu n° 10

SESSION ORDINAIRE DE **2024 - 2025**

Présidence de M. Philippe Latombe, *Président*

– Audition, ouverte à la presse, de représentants de la Commission nationale de l'informatique et des libertés (CNIL) : M. Michel Combot, directeur des technologies, de l'innovation, et de l'intelligence artificielle, M. Victor Nicolle, directeur des contrôles et des sanctions, M. Florent Della Valle, chef du service de l'expertise technologique et Mme Chirine Berrichi, conseillère pour les questions parlementaires et institutionnelles 2

ASSEMBLÉE NATIONALE

La séance est ouverte à 16 heures 35

La commission spéciale a auditionné M. Michel Combot, directeur des technologies, de l'innovation, et de l'intelligence artificielle, M. Victor Nicolle, directeur des contrôles et des sanctions, M. Florent Della Valle, chef du service de l'expertise technologique et Mme Chirine Berrichi, conseillère pour les questions parlementaires et institutionnelles, représentant la Commission nationale de l'informatique et des libertés (CNIL).

M. le président Philippe Latombe. Nous poursuivons nos auditions sur le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, avec l'audition de représentants de la Commission nationale de l'informatique et des libertés (Cnil).

À titre liminaire et à toutes fins utiles, je tiens à indiquer que je suis membre du collège de la Cnil.

Le projet de loi que la commission spéciale est chargée d'examiner comporte trois titres. Le titre I^{er}, consacré à la résilience des activités d'importance vitale, procède à la transposition de la directive sur la résilience des entités critique, dite REC. Mme Catherine Hervieu en est la rapporteure. Le titre II vise à renforcer notre cadre juridique en matière de cybersécurité et procède à la transposition de la directive européenne NIS 2 (*Network and Information Security* 2). Mme Anne Le Hénanff en est la rapporteure. Enfin, le titre III est consacré à la résilience opérationnelle numérique du secteur financier et procède à la transposition du règlement sur la résilience opérationnelle numérique du secteur financier, dit Dora (Digital Operational Resilience Act). M. Mickaël Bouloux en est le rapporteur. Éric Bothorel est le rapporteur général du projet de loi.

Plusieurs dispositions du projet de loi sont relatives à la Cnil.

L'article 17 dispose que l'Agence nationale de la sécurité des systèmes d'information (Anssi) informe la Cnil des incidents ayant un impact important sur la fourniture des services des entités essentielles et importantes ainsi que de certaines administrations, et susceptibles d'entraîner une violation de données à caractère personnel. Cette notification permettra à la Cnil d'exercer ses missions de contrôle et de sanction, conformément au Règlement général sur la protection des données (RGPD).

Les articles 19 et 22 sur les données relatives aux noms de domaine renvoient leurs modalités d'application à deux décrets en Conseil d'État, pris après avis de la Cnil.

L'article 23 encadre les échanges d'informations, notamment entre l'Anssi et la Cnil.

Enfin, l'article 37, alinéa 5, dispose que si les manquements relevés dans le cadre du titre II constituent également une violation du RGPD donnant lieu à une amende administrative prononcée par la Cnil, la commission des sanctions ne peut prononcer de sanction sous forme d'amende administrative. Cette disposition suscite des interrogations, non sur le principe bien connu du *non bis in idem*, mais sur les modalités d'application concrètes des procédures et sur leur articulation.

Dans ce contexte, nous souhaitons vous entendre sur la manière dont vous percevez le projet de loi et sur les éventuels angles morts auxquels il faudrait remédier dans le cadre de

l'examen du texte par l'Assemblée nationale. Je vous laisse la parole pour une intervention liminaire, avant que nos rapporteurs et l'ensemble de nos collègues puissent vous interroger.

M. Michel Combot, directeur des technologies, de l'innovation et de l'intelligence artificielle de la Cnil. Merci, monsieur le président, de nous donner l'occasion de nous exprimer sur ce projet de loi, lié au cœur des activités de la Cnil en matière de cybersécurité.

La Cnil doit veiller au respect de la vie privée et au développement des innovations et des nouveaux services. L'enjeu de la cybersécurité constitue l'une des priorités de la Commission, dont la prérogative principale en la matière est la gestion des incidents liés aux violations de données. Depuis 2018, en application du RGPD, les entreprises ont l'obligation de notifier vols et pertes de données à la Cnil, qui instruit ces incidents et considère, le cas échéant, si les entreprises ont bien appliqué certaines dispositions.

L'augmentation des incidents liés à la cybersécurité s'est traduite par une augmentation des violations de données, dont le nombre a été supérieur à 5 500 en 2024. Plus de 50 % de ces violations sont liées à des actes de piratage, soit des actes volontaires extérieurs, et près de 45 % sont liées à des problèmes rencontrés par l'entreprise. Par ailleurs, plus d'un tiers des incidents concernent des PME.

Du point de vue de la Cnil, le renforcement de la maturité des entreprises dans le domaine de la cybersécurité constitue un enjeu clé, notamment pour la protection des données personnelles détenues par les entreprises. À cet égard, la Cnil ne peut que soutenir l'objectif initial de la directive NIS 2 et de sa transposition dans le droit français. Plus les entreprises seront préparées, mieux elles seront à même de protéger les données de leurs clients et la vie privée de nos concitoyens.

La Cnil accompagne aussi de manière globale le secteur, en édictant les obligations dérivées du RGPD en matière de cybersécurité. À titre d'exemple, en ce qui concerne l'authentification multifacteurs, l'accès en interne doit être très sécurisé pour les grandes bases de données. Nous avons développé un programme de travail pour nous assurer que les bonnes pratiques sont appliquées par les entreprises, en ciblant des secteurs et des tailles d'entreprises correspondants aux violations de données constatées. La cybersécurité est l'une des priorités de notre plan d'action 2025-2028. L'un des enjeux sera d'intégrer les collectivités locales dans le champ des obligations dérivées de la directive NIS 2.

J'en viens au projet de loi, dont l'architecture nous convient. L'articulation de nos activités avec celles de l'Anssi constitue un enjeu. Cependant, nous collaborons déjà au quotidien depuis la création de l'Agence à la fin des années 2000. Cette question de l'articulation se pose pour plusieurs sujets, dont certains font l'objet d'articles du projet de loi et d'autres d'un travail opérationnel.

La transposition de la directive NIS 2 va décupler le nombre d'entreprises concernées par les exigences et les obligations en matière de cybersécurité. À cet égard, un minimum doit être mis en place quant à la protection des données personnelles, en l'adaptant à la capacité des entreprises. L'Anssi travaille à ce calibrage et nous collaborons très bien à ce stade. Le niveau de maturité des entreprises, en particulier les plus petites, et des collectivités locales s'en trouvera amélioré.

J’en viens au sujet de la notification. Le projet de loi prévoit que l’Anssi doit informer la Cnil de certains incidents, ce qui nous convient parfaitement. Pour nous, l’enjeu est d’agir le plus rapidement possible. La notification des violations de données permet d’abord d’informer les concitoyens touchés, afin de prévenir toute fraude ultérieure. La divulgation d’informations, notamment bancaires, peut se révéler très préjudiciable, en particulier pour les populations les plus défavorisées, moins enclines à identifier ce genre de fraudes. Plus la Cnil est informée en amont, mieux elle peut effectuer son travail de contrôle et de prévention des dommages liés aux violations de données.

Les contrôles peuvent être préalables à d’éventuelles sanctions. Le projet de loi garantit la possibilité de faire appel à des experts croisés, ce à quoi nous sommes très favorables. Nous pourrons croiser les expertises lors des contrôles menés par chaque entité : l’Anssi pourra bénéficier d’experts spécialisés dans le domaine de la protection de la vie privée et la Cnil faire appel à des experts de l’Agence.

L’échange d’informations, qui permettra d’améliorer l’efficacité des procédures, fait également l’objet de dispositions dans le projet de loi. Nous avons quelques interrogations concernant leur rédaction, notamment en ce qui concerne la notion d’« intérêts commerciaux des entités concernées ». Sans remettre en cause la nécessaire protection du secret des affaires, cette notion ne semble pas totalement bien définie. Il faudrait la supprimer ou la préciser, pour renvoyer plutôt à des « secrets protégés par la loi », afin de s’assurer que la transmission d’informations a uniquement pour objet des données nécessaires et suffisantes au contrôle et à la mise en place des procédures. Des définitions normées permettront d’éviter des problèmes *a posteriori*, en cas de contestation des procédures.

J’en viens à la coordination des sanctions. L’enjeu ne se situe effectivement pas autour du principe du *non bis in idem*, bien établi dans la jurisprudence, mais autour de l’existence d’un mécanisme qui soit complémentaire et pas surabondant. Au-delà du projet de loi, la coopération quotidienne entre les deux entités sera très importante. Il sera aussi important de prendre de manière complémentaire des mesures préalables aux sanctions, telles que des demandes de mise en conformité et des mises en demeure. Si une sanction doit être prise quand elle est nécessaire, l’objectif reste la mise en conformité. Notre collaboration avec l’Anssi est suffisamment ancienne pour que nous soyons confiants quant à notre capacité à développer une approche conjointe et non concurrentielle. Nous envisageons également de signer une convention.

Le projet de loi fait aussi référence à la stratégie nationale en matière de cybersécurité. La Cnil souhaite en être partie prenante, dans le respect de son indépendance. Notre vision est complémentaire à celle de l’Anssi. *A contrario* de ce qui se passe pour d’autres stratégies nationales, comme celle portant sur l’intelligence artificielle, nous souhaitons jouer toute notre part dans la stratégie de l’État en matière de cybersécurité.

Ce projet de loi nous convient, même s’il peut être amélioré. L’urgence est d’en mettre en œuvre les dispositions, afin d’assurer la nécessaire montée en maturité technologique de certaines entités, notamment les PME et les collectivités. Elles seront accompagnées et auront le temps, mais il leur faut comprendre qu’elles doivent désormais se mettre en conformité. Selon une étude que nous avons récemment publiée, l’application du RGPD au domaine de la cybersécurité aura un impact économique positif pour les entreprises. Les coûts évités pourraient s’élever à plus de 100 millions grâce à une baisse de la fraude. Ce coût évité est un élément important, qui nous conduit aussi à soutenir l’adoption rapide de ce projet de loi.

M. le président Philippe Latombe. La directive NIS 2 prévoit des sanctions, notamment financières. Celles-ci se cumuleraient-elles aux sanctions liées à la non-application du RGPD ? Lors de leur audition, les responsables de l'Anssi nous ont indiqué qu'en cas de fuite des données et de problème de cybersécurité, l'amende relative au RGPD serait retenue, notamment parce qu'elle serait plus élevée.

En cas de fuite de données personnelles, la Cnil est saisie et elle garde la main si un problème de cybersécurité se pose ensuite. *A contrario*, si un problème de cybersécurité survient d'abord et qu'on se rend compte ensuite qu'il a généré une fuite de données, l'Anssi reste-t-elle responsable ou la Cnil reprend-elle la main ? Ce cas est-il déjà prévu ou faut-il l'inclure de façon plus claire dans le projet de loi ?

Au cours de nos auditions, on nous a souvent fait part de la volonté des entreprises de pouvoir accéder à une déclaration commune pour signaler des incidents auprès de l'Anssi, de la Cnil et des autorités de tutelle telles que l'Autorité des marchés financiers (AMF) ou l'Autorité de contrôle prudentiel et de résolution (ACPR) pour l'application de Dora ; qu'en pensez-vous ?

Enfin, la Cnil prend des sanctions à l'encontre des collectivités au titre du RGPD ; pouvez-vous revenir sur votre expérience en la matière ? Nombre des personnes auditionnées ont signalé une différence de traitement entre les entreprises soumises à sanction et les collectivités locales, qui ne le sont pas.

Mme Catherine Hervieu, rapporteure. Les missions de la Cnil continuent de s'étendre, en raison des décisions des législateurs européens et français, mais cette extension advient dans un contexte budgétaire contraint.

Depuis 2024, vous avez dû reporter certains remplacements d'agents et plusieurs nouveaux recrutements, qui étaient pourtant importants pour l'atteinte de vos objectifs. Dans le rapport que vous avez publié en avril 2025, il est écrit que « de nouvelles remises en cause de ses moyens financiers et humains, mettraient en risque la capacité de la Cnil à assurer de manière satisfaisante des missions pourtant essentielles à la préservation des libertés fondamentales de chacun ». À cet égard, comment envisagez-vous l'application de ce projet de loi ?

Les collectivités sont très allantes sur le sujet du numérique, ayant compris l'importance des enjeux de gestion des données pour améliorer leur fonctionnement et des enjeux en matière de cybersécurité. Travailler avec vous représente pour elles une plus-value mais elles butent sur la question de la formation, initiale et continue des agents comme des élus, qui nécessite des moyens et des ressources humaines.

M. Michel Combot. Je comprends le besoin de simplifier les notifications d'incidents, mais le type d'informations remontées varie selon les entités ; la création d'un mécanisme unique ne serait pas neutre. Dans le cas du filtre anti-arnaque par exemple, tout le monde bute sur la question des moyens et du développement d'un système de transmission sécurisée, quand un schéma délocalisé semblerait préférable. Notre procédure est assez simple, fonctionne bien et nous évite d'avoir accès à des informations dont nous n'avons pas besoin, ce qui semble important, notamment au regard de notre objectif de minimisation des données.

Nos enjeux budgétaires ne sont pas propres au domaine de la cybersécurité. À titre d'exemple, l'entrée en vigueur prochaine du règlement sur l'intelligence artificielle posera aussi des questions de moyens.

En 2024, nous avons reçu 17 000 plaintes, dont le traitement est obligatoire au titre du RGPD. Si on les ignore, elles peuvent être contestées et les procédures peuvent remonter jusqu'au Conseil d'État voire jusqu'à la Cour de justice de l'Union européenne.

Une centaine de sanctions ont été prises, dont les deux tiers relèvent de la procédure simplifiée. Les sanctions ont une visée d'exemplarité mais doivent surtout servir à mettre en conformité et à mettre fin au préjudice, ce qui exige un traitement rapide nécessitant suffisamment de moyens.

Les collectivités doivent gagner en maturité et en compétence d'un point de vue technologique dans les domaines de la cybersécurité, de l'intelligence artificielle et de la vidéo. On sent leur volonté de bien faire, mais notre direction chargée de l'accompagnement doit avoir les moyens de mener à bien sa mission.

Les sujets que nous traitons se complexifient et représentent des enjeux forts pour nos concitoyens en matière de violations des données et de libertés. Ainsi, le sujet de l'intelligence artificielle et de la vidéo soulève des questions liées aux libertés publiques.

En ce qui concerne le développement des technologies, nous accompagnons le gouvernement sur les enjeux de protection des données et de souveraineté ; cette expertise requiert aussi des emplois. Nous avons émis nos demandes et sommes en dialogue avec les services de l'État. Il nous faut des moyens adaptés pour répondre à la demande croissante de nos concitoyens en matière de protection et d'accompagnement, pour faire face à des enjeux qui sont au cœur du débat politique.

M. Victor Nicolle, directeur des contrôles et des sanctions de la Cnil. En ce qui concerne les moyens dévolus par la Cnil à la chaîne dite répressive, un peu plus de 50 agents se consacrent aux contrôles et aux sanctions, parmi lesquels une grosse moitié se concentrent sur les contrôles et une petite moitié sur les sanctions. En 2024, nous avons pris 88 sanctions représentant un total de 55 millions d'euros. Environ 70 sanctions relevaient de la procédure simplifiée à juge unique, qui peut donner lieu à des amendes plafonnées à 20 000 euros. Les autres sanctions relevaient de la procédure ordinaire, qui permet d'avoir recours à des amendes plus importantes.

Le principe du *non bis in idem* est inscrit au cinquième alinéa de l'article 37 du projet de loi, avec des limites. Ainsi, si les pouvoirs de la commission des sanctions de l'Anssi sont restreints, ceux de la Cnil en la matière ne le sont pas. De plus, le principe porte sur les sanctions financières qui peuvent être prononcées par l'Anssi, laissant une souplesse pour prendre d'autres mesures correctrices, telles que des mises en demeure ou des rappels aux obligations légales. Ainsi, chaque institution peut mener à bien sa mission : la continuité des activités essentielles pour l'Anssi et la protection des données pour la Cnil.

Nous reconnaissons le besoin d'articulation entre les deux entités, qui figurait dans l'avis de la Cnil du 23 mai 2024. Nous procédons déjà à des échanges substantiels concernant la chaîne répressive. Ainsi, les référentiels de l'Anssi sont utilisés de façon quotidienne par la Cnil lors de ses missions de contrôle et sont visés dans les décisions de sanction adoptées par la formation restreinte de la Cnil, au titre de normes qui s'imposent. De plus, il y a un an, la

Cnil a accueilli des agents de l'Anssi pour effectuer des missions de contrôle. Des éléments de coopération existent, qui auraient vocation à être développés grâce à la coordination envisagée dans le cadre du projet de loi.

La Cnil a appelé à la création d'un mécanisme d'orientation préalable qui pourrait consister, pour l'Anssi, à informer la Cnil de façon systématique lorsqu'elle est saisie d'un incident de cybersécurité mettant en cause des violations de données et, pour la Cnil, à signaler à l'Anssi les violations dont elle aurait connaissance, notamment dans le cadre de sa chaîne répressive. Si les choses sont bien faites au stade des contrôles, l'aiguillage sera bon et les doublons seront évités en matière de sanctions.

Les dispositions de l'article 23, sous réserve de ce qu'a mentionné Michel Combot concernant la formule retenue, permettraient d'asseoir la coordination entre les deux institutions, dans le cadre d'une convention qui reste à écrire mais autour de laquelle les échanges ont débuté.

J'en viens aux collectivités territoriales. Environ 17 % des notifications de violations de données faites à la Cnil concernent des administrations publiques et la moitié d'entre elles sont des collectivités territoriales, qui traitent des données particulièrement sensibles. L'Anssi a également relevé que ces dernières ont subi 14 % des incidents de cybersécurité qui leur ont été notifiés en 2024, soit 218.

La Cnil a déjà prononcé des sanctions à l'égard de collectivités et procède à des contrôles réguliers. Dans la perspective de la montée en régime qu'impose la transposition de la directive NIS 2, elle a fait de la cybersécurité des collectivités l'une de ses thématiques prioritaires de contrôle pour 2025. Ainsi, elle pourra contrôler les mesures organisationnelles et les mesures de sécurité interne mises en place par les collectivités pour sécuriser leurs données. Elle pourra aussi contrôler leurs sous-traitants, ce qui pourra avoir un impact important sur l'ensemble du réseau puisque certains marchés sont dévolus à seulement deux ou trois d'entre eux.

Les sanctions prononcées par la Cnil à l'encontre des collectivités territoriales tiennent compte de leurs moyens, selon les prescriptions du RGPD. Elles sont adaptées à l'objectif de mise en conformité des acteurs et peuvent prendre la forme de mises en demeure.

Mme Chirine Berrichi, conseillère pour les questions parlementaires et institutionnelles de la Cnil. Je voudrais apporter une précision quant à l'impact des décisions de la Cnil sur les collectivités territoriales. En 2022, nous avons prononcé des mises en demeure à l'encontre de vingt-deux communes de plus de 20 000 habitants. Dans les trois mois qui ont suivi, nous avons enregistré 2 000 désignations de délégués à la protection des données, qui visaient à répondre au manquement reproché à ces communes. Ces mesures répressives ont donc un effet dissuasif et d'entraînement.

M. le président Philippe Latombe. Nous en venons aux questions des autres députés.

M. Antoine Villedieu (RN). Le projet de loi prévoit que les agents de l'État pourront accéder sans autorisation judiciaire préalable aux locaux, aux documents, aux données informatiques, voire aux informations protégées par le secret professionnel des opérateurs d'importance vitale. Ces pouvoirs, notamment inscrits aux articles R. 1332-12 et suivants du

code de la défense, s'appliqueraient à des entreprises privées, à des établissements publics et même à des collectivités territoriales.

Une telle extension du pouvoir administratif sans encadrement judiciaire clair n'ouvre-t-elle pas la voie à un déséquilibre profond entre exigence de sécurité et respect des libertés fondamentales ?

Comment la Cnil évalue-t-elle ce glissement, qui pourrait faire peser une menace sur la confidentialité des échanges ou la protection des données personnelles, dans des secteurs pourtant soumis à des obligations déontologiques ou professionnelles très strictes ?

Enfin, que pensez-vous de l'introduction de garanties juridictionnelles, ne serait-ce que d'un contrôle *a posteriori*, pour éviter que la sécurité numérique ne devienne un prétexte à une surveillance administrative généralisée ?

M. Victor Nicolle. Vous évoquez les pouvoirs de l'Anssi, que nous ne sommes pas les mieux placés pour commenter.

En ce qui concerne les contrôles conduits par la Cnil, la loi « informatique et libertés » prévoit une obligation de coopération de la part des acteurs à contrôler, qu'ils soient publics ou privés. Les contrôles qui ont lieu dans les locaux des entreprises peuvent faire l'objet d'un refus, que la Cnil et les agents en charge du contrôle peuvent outrepasser en saisissant le juge des libertés et de la détention. Ce cas de figure est peu fréquent et, en général, les entreprises collaborent aux contrôles.

Quant aux secrets, ils sont encadrés par la loi « informatique et libertés ». De plus, les agents de la Cnil sont soumis à une obligation de confidentialité.

M. Michel Combot. Toutes les décisions et procédures de la Cnil sont sous le contrôle du juge administratif et peuvent être contestées, tant sur le fond que sur la forme. Ce sera sûrement le cas aussi pour les procédures de l'Anssi, qui devront répondre aux mêmes obligations en matière de déontologie et garantir que seules les informations nécessaires et suffisantes sont collectées. L'activité des entités procédant à des sanctions administratives est encadrée et une jurisprudence existe dans ce domaine. En matière de protection des libertés des individus et des entreprises, des garde-fous suffisants sont en place.

M. le président Philippe Latombe. L'existence de sanctions à l'encontre des collectivités, même si vous n'y avez pas recours, vous semble-t-elle nécessaire pour que le dispositif fonctionne ? La question nous a été posée. Le Conseil d'État répond qu'on ne peut prévoir des sanctions pour le secteur privé sans en prévoir pour la sphère publique. Selon certains, puisque les collectivités ont le désir de monter en expertise et en maturité en matière de cybersécurité, les sanctions ne sont pas nécessaires. Selon d'autres, sans sanctions les collectivités seraient moins allantes. Pensez-vous qu'il soit possible de fonctionner sans sanctions ? S'il faut en prévoir, de quel type de sanctions doit-il s'agir ? Des plans de remédiation comme vous en mettez en place sont peut-être plus efficaces que des sanctions administratives pécuniaires.

M. Michel Combot. La nature et le montant des sanctions de la Cnil sont adaptés au préjudice subi et au chiffre d'affaires de l'entité sanctionnée. Le quantum s'appliquant aux collectivités est donc forcément différent. Je le répète : nous recherchons d'abord la remise en conformité. La sanction, qui a un caractère dissuasif, tombe notamment si un acteur a

bénéficié d'une situation illégale. Il est difficile de dire si les choses fonctionneraient aussi bien sans sanctions ; il s'agit d'une question éminemment politique, à laquelle il vous revient de répondre.

M. le président Philippe Latombe. Le RGPD prévoyait explicitement le cas de figure, ce qui était plus simple.

M. Victor Nicolle. Il faut entendre la sanction de façon large et ne pas se limiter à la procédure de sanction diligentée devant la formation restreinte de la Cnil. À titre d'exemple, pour des acteurs publics qu'on ne peut pas sanctionner financièrement, les mises en demeure, qui peuvent être rendues publiques, peuvent constituer une incitation très forte à se remettre en conformité. La sanction n'est pas la panacée et la sanction financière n'est pas le seul levier dont dispose la Cnil.

M. Antoine Villedieu (RN). Que pensez-vous de l'absence de garantie contre la sous-traitance hors Union européenne des services essentiels ? Je pense aux data centers, aux clouds critiques et aux réseaux.

M. Michel Combot. La question est de savoir quelles sont les données dont il s'agit et par qui elles sont détenues. Il y a un enjeu de souveraineté. Nous soutenons pleinement la stratégie du gouvernement sur le « cloud au centre », qui a été notamment transposée par la loi, visant à sécuriser et à réguler l'espace numérique, dont nous attendons des décrets d'application sur lesquels la Cnil donnera son avis.

Il s'agit d'une question politique et c'est à l'État de décider quelles sont les données soumises à un type particulier de protection. Du point de vue la Cnil, la protection de la vie privée est importante et certaines données, notamment sensibles, doivent pouvoir être écartées de l'accès extraterritorial par des pays situés hors de l'Union européenne. La définition du champ de ces données revient à l'État, notamment quand ce dernier les détient.

Pour les entreprises, dans le domaine bancaire par exemple, nous recommandons que les entreprises puissent se saisir de ce sujet important. Les solutions technologiques à appliquer ne sont pas simples ; les développer constitue un enjeu collectif, auquel la Cnil prend toute sa part.

M. le président Philippe Latombe. Le projet de loi devrait être examiné en séance au mois de septembre, ce qui nous laisse du temps. Si des sujets n'ont pas été abordés aujourd'hui, n'hésitez pas à nous faire parvenir une contribution écrite. Le but est de clarifier le plus possible le projet de loi afin de le rendre efficace et relativement accessible pour les entreprises et les administrations. Le champ de la directive NIS 2 est large et de nombreux nouveaux acteurs vont être confrontés à la mise conformité ; nous avons besoin de faire les choses le plus sereinement possible.

La séance est levée à 17 heures 20

Membres présents ou excusés

Commission spéciale chargée d'examiner le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité

Réunion du mardi 10 juin 2025 à 16 h 35

Présents. - Mme Catherine Hervieu, M. Philippe Latombe, M. Vincent Thiébaut, M. Antoine Villedieu

Excusé. - M. Mickaël Bouloux